

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

01/08/2013

SUBJECT:

Vulnerability in Adobe Flash Player Could Allow For Remote Code Execution (APSB13-01)

OVERVIEW:

A vulnerability has been discovered in Adobe Flash Player that could allow an attacker to take control of the affected system. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

SYSTEMS AFFECTED:

Adobe Flash Player 11.5.502.135 and earlier versions for Windows
Adobe Flash Player 11.5.502.136 and earlier versions for Macintosh
Adobe Flash Player 11.2.202.258 and earlier versions for Linux
Adobe Flash Player 11.1.115.34 and earlier versions for Android 4.x
Adobe Flash Player 11.1.111.29 and earlier versions for Android 3.x and 2.x
Adobe AIR 3.5.0.880 and earlier versions for Windows, Adobe AIR 3.5.0.890 and earlier versions for Macintosh and Adobe AIR 3.5.0.880 for Android
Adobe AIR 3.5.0.880 SDK and Adobe AIR 3.5.0.890 SDK

RISK:

Government:

Large and medium government entities: **High**
Small government entities: **High**

Businesses:

Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:

Adobe Flash Player is prone to a vulnerability that could allow for remote code execution. Adobe has released security updates for Adobe Flash Player 11.5.502.135 and earlier versions for Windows, Adobe Flash Player 11.5.502.136 and earlier versions for Macintosh, Adobe Flash Player 11.2.202.258 and earlier versions for Linux, Adobe Flash Player 11.1.115.34 and earlier versions for Android 4.x, and Adobe Flash Player 11.1.111.29 and earlier versions for Android 3.x and 2.x.

Flash Player installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 11.5.31.137 for Windows, Macintosh and Linux. Flash Player installed with Internet Explorer 10 for Windows 8 will automatically be updated to the latest Internet Explorer 10 version, which will include Adobe Flash Player 11.3.378.5 for Windows.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

Install the updates provided by Adobe immediately after appropriate testing.

Users of Adobe Flash Player 11.5.502.135 and earlier versions for Windows should update to Adobe Flash Player 11.5.502.146.

Users of Adobe Flash Player 11.5.502.136 and earlier versions for Macintosh should update to Adobe Flash Player 11.5.502.146.

Users of Adobe Flash Player 11.2.202.258 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.261.

Users of Adobe Flash Player 11.1.115.34 and earlier versions on Android 4.x devices should update to Adobe Flash Player 11.1.115.36.

Users of Adobe Flash Player 11.1.111.29 and earlier versions for Android 3.x and earlier versions should update to Flash Player 11.1.111.31.

Users of Adobe AIR 3.5.0.880 and earlier versions for Windows and Macintosh should update to Adobe AIR 3.5.0.1060.

Users of the Adobe AIR SDK (includes AIR for iOS) should update to the Adobe AIR 3.5.0.1060 SDK.

Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.

Do not open email attachments from unknown or untrusted sources.

REFERENCES:

Adobe:

<http://www.adobe.com/support/security/bulletins/apsb13-01.html>

SecurityFocus:

<http://www.securityfocus.com/bid/57184>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0630>